

OFFICE OF THE DIRECTOR  
DEPARTMENT OF MOTOR VEHICLES  
Audits Office  
P.O. BOX 932328 MS H-230  
SACRAMENTO, CA 94232-3280



October 20, 2009


Joan Obert, Director  
State Department of Child Support Services  
PO Box 419064  
Rancho Cordova, CA 95741

File No: C-97-9055

Dear Ms. Obert:

The Department of Motor Vehicles' (DMV) Audits Office presents its final audit report of the State Department of Child Support Services State Office (State DCSS) Audit for March 2008 – March 2009. The audit report entitled "*Final Audit Report – State Department of Child Support Services State Office Audit*" is attached for your information. Please note the attached report includes excerpts of State DCSS response to our findings, as well as our evaluation to your response. We have included the response received from State DCSS in its entirety as an attachment at the end of the report.

We thank State DCSS and their staff during this review for their cooperation and courtesy extended to our auditors. If you have any questions please contact me at (916) 657-5828.

  
**GRACE M. RULE-ALI, Manager**  
Information Systems-Requester Audit Section

Attachment

cc: Debbie Martin, Information Security Officer, State DCSS  
Jim Woodward, Chief, ISB  
Tam Le, Manager, ISB Policy & Information Privacy Section

FINAL AUDIT REPORT  
CALIFORNIA DEPARTMENT OF MOTOR VEHICLES  
EXECUTIVE AUDITS  
STATE DEPARTMENT OF CHILD SUPPORT SERVICES

TABLE OF CONTENTS

COVER MEMO .....	i
EXECUTIVE SUMMARY.....	1
BACKGROUND .....	1-2
OBJECTIVES, SCOPE, AND METHODOLOGY .....	2-3
FINDINGS AND RECOMMENDATIONS.....	3
FINDING#1 SECURITY STATEMENTS VIOLATION – FAILURE TO MAINTAIN INFORMATION SECURITY STATEMENTS FOR EMPLOYEES.....	3
FINDING #2 INADEQUATE/LACK OF DOCUMENTATION – FAILURE TO MAINTAIN SUPPORTING DOCUMENTATION FOR DMV INQUIRIES .....	3-4
CONCERN.....	4
CONCLUSION.....	4-5
EXHIBIT 1: STATE DCSS RESPONSE.....	6

## **EXECUTIVE SUMMARY**

The California Department of Motor Vehicles (DMV) Information Services Branch (ISB) operates an information requester program that allows external entities to access DMV records pursuant to applicable statutes of the California Vehicle Code (CVC) and California Code of Regulations Title 13, Article 5 except as prohibited by CVC Section 1808.21. As an authorized DMV Government Requester Account holder the State Department of Child Support Services State Office (State DCSS), has access to basic record, address and social security information on California Driver License and Vehicle Registration. In accordance with its DMV Government Requester Account agreement, State DCSS is allowed to make California DMV inquiries for its business needs.

The CVC mandates that DMV protect the privacy rights of the public by releasing only certain information authorized by statutes. Statutes and regulations allow for businesses and individuals to access DMV records containing both confidential and non-confidential information, contingent upon approval of an application and compliance with the program requirements. DMV is dedicated in its mission of securing personal information for consumer protection. To meet our obligation of protecting the public and DMV information, we reviewed State DCSS compliance with the DMV Government Requester Account stipulations, and applicable California laws and regulations.

Our evaluation found that the current security controls in effect at State DCSS as of July 22, 2009, are sufficient to meet the security objectives of this audit.

## **BACKGROUND**

The State DCSS has responsibility for the county and regional child support agencies that serve approximately 1.8 million children. State DCSS services include, but are not limited to, locating parents, establishing paternity, establishing, modifying and enforcing a court order for child support. State DCSS monitors local child support agencies (LCSAs) compliance within the Child Support Program. This context refers to LCSA's adhering to and/or meeting State and Federal mandated requirements. Generally the requirements are expressed in terms of the quantity or quality of effort, required timeframe, and/or other mandatory measurable expectations. These requirements govern identified actions LCSAs must take and set specific time frames for those various actions when managing child support cases.

In June 2002 statutory changes reshaped the California child support program. The LCSA's were no longer considered law enforcement agencies and had to change the access methods to obtain DMV data. Formerly, LCSA requested access to DMV's databases via CLETS. The statutory changes caused LCSAs to obtain an alternate method of access. Effective July 1, 2002, due to the June statutory changes, DMV granted approval to allow Computer Assisted Support Enforcement System (CASES) Consortium electronic access to data from its files via the existing Health and Human Services Data Center. The CASES Consortium was comprised of a grouping

of LCSAs. DMV's approval was granted with the condition that the CASES Consortium member agencies were to have the appropriate access, logging and auditing controls are in place.

While the State DCSS was responsible for overseeing the CASES Consortium county member agencies in this process, the CASES Consortium was disbanded effective June 30, 2009. This change requires county agencies, who wish to do so, obtain a new method for on-line access, or rely on the existing overnight batch processing to receive DMV information.

DMV granted approval to allow the State DCSS office batch access via the Offices of Technology Services (OTech), formerly the Department of Technology Services. This approval was also granted with the condition that the appropriate access, logging and auditing controls are in place. The State DCSS requester code has the following access to DMV information:

- Driver License – to help determine physical descriptions, addresses and age of subjects suspected of welfare fraud.
- Vehicle Registration – to help verify vehicles owned, and to verify place of residence of those suspected of welfare fraud.
- Social Security Number Information.

### **OBJECTIVES, SCOPE, AND METHODOLOGY**

DMV is responsible for administering statewide programs that use and rely on information assets whether they are electronically stored or hard copy documents. DMV conducts audits and evaluations of entities accessing the information of the Department, for compliance purposes. The audit was performed in accordance with *Government Auditing Standards*, Generally Accepted Auditing Standards, and the California Department of Motor Vehicles' Government Requester Account Requirements.

The audit objectives were to verify compliance with the requirements of the requester accounts held by State DCSS, as well as applicable statutes and regulations stated in the CVC and the California Code of Regulations; and review the security procedures that State DCSS has in place to ensure the protection of DMV information. This included evaluation of State DCSS administrative procedures, and applicable monitoring programs.

Our evaluation methodology included such tests as considered necessary to meet our objectives. Interviews were conducted with State DCSS management to determine the levels of security, and confidentiality over DMV information.

We conducted the audit fieldwork at the State DCSS office in Sacramento, California April 28, 2009. Our audit included an examination of the administrative security procedures, and the monitoring of programs that are in place to protect DMV information. During the entrance conference, DMV was informed that State DCSS had employees who were previously assigned to work at the Franchise Tax Board (FTB) Office. The employees used FTB's communication interface with DMV to make DMV inquiries. In January 2008 the Audits Office conducted an audit of FTB, and issued a no finding report. Based on this review DMV relied on the

information system security portion of the FTB audit for verification of the system's security that was used by State DCSS employees to process DMV inquiries. These areas were not reviewed in this audit.

## **FINDINGS AND RECOMMENDATIONS**

### **FINDING #1: SECURITY STATEMENTS VIOLATION – FAILURE TO MAINTAIN INFORMATION SECURITY STATEMENTS FOR EMPLOYEES**

**Condition:** The State DCSS did not maintain Information Security Statements (INF 1128), for all DMV requester account users. State DCSS employees, and/or system administrators with direct or indirect access to DMV information must sign statements, and recertify annually. The security statements record that State DCSS employees are informed to restrict the use and knowledge of requester codes, operational manuals, and DMV information to those who are authorized.

**Criteria:** The Memorandum of Understanding Memorandum of Understanding (MOU) # 9 states, "Requester agrees to establish security procedures to protect the confidentiality of DMV records and access information, as required by California Vehicle Code Section 1808.47. Requester shall ensure that each Requester's employee or each person working on behalf of Requester having direct or incidental access to DMV records have signed an individual security statement. That statement shall contain, at a minimum, the same provisions contained within the DMV's Information Security Statement, form INF 1128. The form shall be maintained on file, and made available to DMV upon request".

**Recommendation:** State DCSS should develop policies and procedures to ensure that all employees with direct and incidental access to DMV records information sign and maintain at worksite, INF 1128, and recertify annually.

**State DCSS Response:** "...The DCSS-Information Security Office (ISO) has modified its manner of ensuring compliance with the requirements for the INF 1128...The signing of this statement is now a part of annual security and privacy awareness training..."

**Audit Office Response:** We concur with State DCSS corrective action implemented.

### **FINDING #2: INADEQUATE/LACK OF DOCUMENTATION**

**Condition:** The State DCSS failed to provide supporting documents for the selected transactions. The State DCSS did not provide any support documentation for DMV inquiries they made. Test transactions were judgmentally selected from requests for the period March 2008 thru March 2009.

**Criteria:** California Code of Regulations Section 350.50(a) states "Each requester code holder shall keep the records retained pursuant to Sections 350.48 and 350.18(b) (4) at the business address listed on the requester code holder's application for a requester code." The Commercial

Requester Information Handbook, Chapter Two, Part II, Security Requirements, Paragraph 2 states "Requester shall maintain the security and integrity of any information it received and shall maintain records and documents to justify and support proper use of requested information. All Requesters are required to establish and maintain daily logs and source document that track the receipt, use and dissemination of DMV information."

**Recommendation:** The State DCSS should maintain supporting documentation to show evidence of proper use of DMV information for all inquiries made. The State DCSS should develop procedures to ensure that all employees with direct and incidental access to DMV records are aware that support documents must be maintained for all DMV inquiries made.

**State DCSS Response:** "...the DCSS-ISO has established logging procedures consistent with DMV Security Requirements, Section A...established procedures for each office with DMV access to forward these logs monthly to the DCSS-ISO. Activity recorded in these logs is matched against activity recorded by the computer systems used to access the DMV database. Any discrepancy between the two logs will be followed up by DCSS-ISO staff...the DCSS-ISO is developing a 'procedure manual' describing how DMV data shall be accessed, used, managed and stored...We are expecting to finalize in October 2009..."

**Audit Office Response:** We concur with State DCSS corrective action plan. To evidence compliance in this area we ask that State DCSS submit a copy of their procedure manual describing how DMV data shall be accessed, used, managed, and stored at a six month follow up.

## CONCERN

The State DCSS information security program needs to include procedures for handling DMV records with a Department of Justice Stop "DOJ Stop" message. There are no documented procedures for handling records with a "DOJ Stop" message. Employees should be educated and procedures should be developed to give employees proper guidance of handling DMV records with a "DOJ Stop" message.

Furthermore, the State DCSS information security program needs to include policies and procedures that address audit log failure. Employees do not have documented procedures to follow in the event the audit log fails to capture user activity. Policies and procedures should be developed to ensure system generated audit records that collect relevant information to identify record access information is not lost in the event of an audit log failure.

## CONCLUSION

The State DCSS operates a system and program that permits its authorized end users access to DMV information, and provides assurance that access to the information is appropriately controlled and monitored in accordance with the requirements of its Government Requester Accounts. Accordingly, the mechanisms and controls in place to protect information received from DMV taken as a whole are sufficient and functioning properly to fulfill the program

objectives. However, because of inherent limitations in control systems, errors or irregularities may occur and not be detected. Consequently, projection of any evaluation of systems to future periods is subject to risk since procedures may become inadequate because of changes, or the degree of compliance with procedures may deteriorate.

Finally, this report identifies areas where State DCSS can improve its level of security over DMV information and help bring the organization closer to compliance with the requirements of the requester accounts held by State DCSS. Implementing the report's recommendations should result in a more effective control of securing and protecting the public's personal and confidential information.



**GRACE M. RULE-ALI, MANAGER**

Information Systems-Requester Audit Section  
Audits Office  
(916) 657-5828

October 20, 2009

**Review Team:**

Carolyn Manuel, Auditor In-Charge  
Benedicta Ikhalo, Auditor  
Andrew Lau, Auditor

**EXHIBIT 1**  
**State DCSS Response**



**CALIFORNIA DEPARTMENT OF CHILD SUPPORT SERVICES**

P.O. Box 419064, Rancho Cordova, CA 95741-9064



October 7, 2009

Ms. Carolyn Manuel, Auditor  
Department of Motor Vehicles  
2570 24<sup>th</sup> Street, Mail Station H121  
Sacramento, California 95818

SUBJECT: RESPONSE TO DMV AUDIT REPORT – AUDIT FILE C-97-9055

Dear Ms. Manuel:

In response to the following findings from this report:

1. Security Statements. The audit found that Department of Child Support Services (DCSS) could not provide INF1128 forms (or equivalent) for all individuals with user IDs to the DMV databases.

The DCSS-Information Security Office (ISO) has modified its manner of ensuring compliance with the requirements for the INF 1128 and other 'acknowledgement of use' forms. The DCSS-ISO has incorporated all language from all such forms into a single acknowledgement statement. The signing of this statement is now a part of annual security and privacy awareness training. Additionally, the annual training, commencing with the 2009 cycle, is delivered using 'computer based training' (CBT), with the signing of the form being incorporated into the training program. A database is used to record the name and date of each individual completing the training.

2. Lack of supporting documents to document DMV inquiries. The audit found that DCSS employees with authorized access to DMV's database were not maintaining the necessary access logs for queries made into DMV's data.

The DCSS-ISO has been given responsibility to oversee and administer all DMV access in child support offices, including DCSS offices. As a part of this effort, the DCSS-ISO has established logging procedures consistent with DMV Security Requirements, Section A. To ensure compliance with these requirements, the DCSS-ISO has also established procedures for each office with DMV access to forward these logs monthly to the DCSS-ISO. Activity recorded in these logs is matched against activity recorded by the computer systems used to access the DMV database. Any discrepancy between the two logs will be followed up by DCSS-ISO staff. Additionally, the DCSS-ISO is developing a 'procedure manual' describing how DMV data shall be accessed, used, managed, and stored. This manual is in draft. A copy will be provided upon request when it is finalized. We are expecting to finalize in October 2009.

Ms. Carolyn Manuel  
October 7, 2009  
Page 2

Please let me know if these corrective actions are adequate. Protecting the information assets we use to do our jobs is very important to DCSS. We appreciate the opportunity to work with you to identify ways we can better protect those assets.

If you have any questions or concerns regarding this matter, please contact me at (916) 464-5774.

Sincerely,

A black rectangular redaction box covering the signature of Deborah Martin.

DEBBORAH MARTIN  
Chief Information Security Officer

cc: Robert Jones, Deputy Director, Operations Division  
Barbara Owens, Audits Manager